IN THE SPECIFICATION:

Please replace paragraph 14 on page 5 with the following paragraph.

~~Figure 5 illustrates~~ **Figures 5A and 5B** illustrate session 500 of the invention;

Please replace paragraph 15 on page 5 with the following paragraph.

~~Figure 6 illustrates~~ **Figures 6A and 6B** illustrate session 600 of the invention;

Please replace paragraph 53 on page 18 with the following paragraph.

~~Figure 5 illustrates~~ **Figures 5A and 5B** illustrate session 500 of the invention. Session 500 may include secure key exchange for identification and authentication where Alice 502 may be the final verifier. Secure key exchange may be viewed as verifying a session key after an initial public key exchange. Moreover, identification may be viewed as establishing identity and authentication may be viewed as verifying identity.

Please replace paragraph 109 on page 37 with the following paragraph.

~~Figure 6 illustrates~~ **Figures 6A and 6B** illustrate session 600 of the invention. Recall that session 500 may include secure key exchange and authentication where Alice 502 may be the final verifier. Session 600 of ~~Figure 6~~ **Figures 6A and 6B** may include secure key exchange and authentication where Bob 604 may be the final verifier.

Please replace paragraph 115 on page 39 with the following paragraph.

At step 634, Alice 602 may encrypt random number N_A 622 with password P_A 606 to obtain encrypted random nonce $(N_A)_{P_A}$ 634. Alternatively, Alice 602 may superencrypt random number N_A 622 with password P_A 606 and at least one other variable known to both Alice 602 and Bob 604 or perform other encryption variations on random number N_A 622 and password P_A 606 as discussed in connection with step 550 and step 552 of ~~Figure 5~~ **Figure 5A**.

Please replace paragraph 116 on page 39 with the following paragraph.

Encrypting random number N_A 622 with password P_A 606 works to accelerate the key verification phase so that the key verification phase may start with Alice 602 of ~~Figure 6~~ **Figures 6A and 6B** rather than Bob 504 of ~~Figure 5~~ **Figures 5A and 5B**.

Please replace paragraph 120 on page 40 with the following paragraph.

At step 640, Bob 604 may obtain password P_B 614 and identity 616 from his user list based on identity 608 received from Alice 602 over transmission 636. The discussion in connection with password P_B 514 of ~~Figure 5~~ **Figure 5A** also applies to password P_B 614 of ~~Figure 6~~ **Figure 6A**.

Please replace paragraph 121 on pages 40-41 with the following paragraph.

At step 640, Bob 604 may verify that identity 608 received from Alice 602 equals identity 616 as obtained from Bob's user list. If identity 608 does not equal identity 616 at step 640, Alice 602 may be an invalid user as far as Bob 604 may be concerned and Bob 604 may proceed to step 644. At step 644, Bob 604 may end session 600 at step 646 or continue with session 600 and generate random password P_B 648 at step 648. The discussion in connection with step 542 of ~~Figure 5~~ **Figure 5A** also applies to step 648 of ~~Figure 6~~ **Figure 6A**.

Please replace paragraph 124 on page 41 with the following paragraph.

At step 656, Bob 604 may employ a combining function, f_B, on password P_B 614 (or password P_B 648) and on the key exchange pieces of Alice's public key M_A 630 and Bob's public key M_B 632 to generate high-entropy secret S_B 656. The discussion in connection with step 548 of ~~Figure 5~~ **Figure 5A** is applicable to step 656 of ~~Figure 6~~ **Figure 6A**. In other words, Bob 604 may employ alternate embodiments with different combining functions as discussed in connection with step 548 of session 500. Steps 652, 654, and 656 may be performed in any order.

Please replace paragraph 125 on page 42 with the following paragraph.

At step 658, Bob 604 may modify N_A 652 to obtain modified random number N_A+1 658. The discussion on modification techniques in connection with step 564 of ~~Figure 5~~ **Figure 5A** is applicable to step 658 in ~~Figure 6~~ **Figure 6A**.

Please replace paragraph 126 on page 42 with the following paragraph.

After modifying N_A 652 received from Alice 602 over transmission 636, Bob 604 may superencrypt his random number N_B 628, and Alice's modified random number N_A+1 658, first with high-entropy secret S_B 656 at step 660, then with session key K_B 654 at step 662 to produce the result

$$((N_B, N_A+1)_S)_K \qquad (662).$$

The alternative encryption embodiments discussed in connection with step 586 and step 588 of ~~Figure 5~~ **Figure 5B** apply to steps 660 and 662 of ~~Figure 6~~ **Figure 6A** as well.

Please replace paragraph 129 on pages 42-43 with the following paragraph.

Alice 602 next may employ the combining function, f, to generate Alice's version of the high-entropy secret. At step 668, Alice may combine password P_A 606 with Alice's public key M_A 630 and Bob's public key M_B 632 to produce high-entropy secret S_A 668. Similar to step 558 of ~~Figure 5~~ **Figure 5A**, if the function and variables employed by Alice 602 in step 668 to produce high-entropy secret S_A 668 are the same as employed by Bob 604 in step 656 to produce high-entropy secret S_B 656, then S_A 668 will equal S_B 656

such that this common high-entropy secret is shared by both Alice 602 and Bob 604.

Please replace paragraph 136 on pages 44-45 with the following paragraph.

Alternative to proceeding to step 679, Alice 602 may proceed to step 681 and continue to work towards establishing a mutually secure two way communication channel with Bob 604. At step 681, Alice 602 may generate initialization vector I_A 681. Alice 602 then may modify random number N_B 672 at step 682. Again, as with step 564 of ~~Figure 5~~ **Figure 5A**, Alice 602 may modify random number N_B 672 in any way that Bob 604 and Alice 602 previously agreed upon.

Please replace paragraph 137 on page 45 with the following paragraph.

Alice 602 may then superencrypt initialization vector I_A 681 and modified random number N_B+1 682, first with the high-entropy secret S_A 668 at step 683, and then with session key K_A 665 at step 684 to produce the result,

$$((I_A, N_B+1)_S)_K \qquad (684).$$

The alternate encryption embodiments discussed in connection with steps 566 and 568 of ~~Figure 5~~ **Figure 5A** also apply to steps 683 and 684 of ~~Figure 6~~ **Figure 6B**. At step 685, Alice 602 may transmit the result $((I_A, N_B+1)_S)_K$ 684 to Bob 604.

Please replace paragraph 138 on page 45 with the following paragraph.

At step 686, Bob 604 may decrypt Alice's superencrypted payload $((I_A, N_B+1)_S)_K$ 684 to extract initialization vector I_A 687 and modified random number N_B+1 688. Bob 604 may next verify at step 690 whether modified random number N_B+1 688 received from Alice 602 over transmission 685 less its modification is equal to Bob's random number N_B 628. If modified random number N_B+1 688 less its modification is not equal to Bob's random number N_B 628, Bob 604 may terminate session 600 at step 692. As was the case in the discussion with reference to step 579 of ~~Figure 5~~ **Figure 5A**, in a hapless case, Bob 604 will remember between steps 648 and 690 that Alice 602 is an invalid user and may accordingly terminate the session at step 692.

Please replace paragraph 141 on pages 46-47 with the following paragraph.

Embodiment 500 of ~~Figure 5~~ **Figures 5A and 5B** may be used in situations where it may be more important for the server to have the first opportunity to break off communications, such as a false client situation. For example, servers hosting web pages of ebay.com, yahoo.com, the United States White House, the United States Pentagon, presidential candidates, and radio talk show hosts may want to employ embodiment 500 so as to have the first opportunity to break off communications (step 580 of ~~Figure 5~~ **Figure 5A**) during repeat attacks that attempt to overload these web sites with requests so as to shut them down.

Please replace paragraph 142 on page 47 with the following paragraph.

Session 500 of ~~Figure 5~~ **Figures 5A and 5B** may be based on the Diffie-Hellman key exchange. However, any suitable key exchange protocol will work. For example, Fast Elliptical Encryption (FEE - see U.S. 5,463,690, U.S. 5,159,632, and U.S. 5,271,061), Communications Setup (COMSET), Shamir's three-pass protocol, and Tatebayashi-Matsuzaki-Newman key exchange algorithms may be substituted for the Diffie-Hellman key exchange in session 500. Substituting a different key exchange protocol may involve replacing the computations of steps 526, 528, 546, and 556 with those computations applicable to the particular protocol.

Please replace paragraph 143 on page 47 with the following paragraph.

Embodiment 600 of ~~Figure 6~~ **Figures 6A and 6B** may be used in situations where it may be more important for the client to have the first opportunity to break off communications, such as a false server situation. For example, a server hosting an electronic store may want to employ embodiment 600 to allow their customers passing their credit card number over the Internet to have the first opportunity to break off communications (step 678 of ~~Figure 6~~ **Figure 6A**). This may instill in the customer a greater sense of security in conducting transactions over the Internet.

Please replace paragraph 144 on pages 47-48 with the following paragraph.

One of the advantages of session 600 is that session 600 includes three transmissions over transmission network 603, which is two network transmissions less than Diffie-Hellman key exchange 200/verification 300 of **Figure 2** and **Figure 3** above. Moreover, although ~~**Figure 6**~~ **Figures 6A and 6B** incorporate aspects of the Diffie-Hellman key exchange, any suitable key exchange protocol may be substituted into ~~**Figure 6**~~ **Figures 6A and 6B**. This may require appropriate substitutions in the computations of steps 630, 632, 654, and 665.

Please replace paragraph 146 on page 48 with the following paragraph.

In the above client-server model embodiments of ~~**Figure 5**~~ **Figures 5A and 5B** and ~~**Figure 6**~~ **Figures 6A and 6B**, Alice may represent a client seeking to authenticate to Bob to request services. However, Bob may be a client and Alice may be a server so that server-client models, server-server models, or client-client models also are encompassed within the scope of the subject matter of the claimed terms. Employing more than two parties per model (such as including at least one the parties of Carol and Dave) also may be encompassed within the scope of the subject matter of the claimed terms.

Please replace paragraph 149 on page 50 with the following paragraph.

Web server system 716 may be at least one computer system that operates as a server computer system and may be configured to operate with the protocols of World Wide Web 702 as part of Internet 700. For example, web server system 716 may be server Bob 504 of ~~**Figure 5**~~ **Figures 5A and 5B** or server Bob 604 of ~~**Figure 6**~~ **Figures 6A and 6B**. Optionally, Web

server system 716 of **Figure 7** may be part of an ISP that provides access to World Wide Web 702 client systems. Web server system 716 may be coupled to server computer system 718, where server computer system 718 itself may be coupled to other devices, such as order form 711. Order form 711 may involve putting together a shopping order for consumer products.

Please replace paragraph 156 on page 53 with the following paragraph.

Memory 806 may be dynamic random access memory (DRAM) and may also include static RAM (SRAM) and read-only memory (ROM). Within memory 806 may be executable programs 807. Memory 806 may be a distributed readable storage medium containing executable computer program instructions which, when executed, cause at least one of a client computer system and a server computer system to perform a key exchange and authentication as set out in ~~**Figure 5**~~ **Figures 5A and 5B** or ~~**Figure 6**~~ **Figures 6A and 6B**. Memory 806 also may be a computer readable storage medium containing executable computer program instructions which, when executed, cause server computer system 718 to perform a key exchange and authentication as set out in ~~**Figure 5**~~ **Figures 5A and 5B** or ~~**Figure 6**~~ **Figures 6A and 6B**.